System Safety for Highly Distributed Air Traffic Management

Nancy Leveson, MIT
Chris Wilkinson, Honeywell

The next generation of air traffic management (called NextGen in the U.S. and SESAR in Europe) will include increased coupling and interconnectivity among airborne, ground, and satellite systems and intensive use of computers and software in safety-critical roles. Control will be shifting from the ground to the aircraft and to shared responsibility for safety among ATC (air traffic control), pilots, and airline operations centers. The planned coupling and interconnection between land, airborne, and satellite systems introduces more potential for accidents stemming from unsafe and unintended component interactions.

NextGen's success will lie in the program's ability to design new ATM (Air Traffic Management) operational increments that do not decrease the safety of the current system. One of the requirements for achieving this goal is the ability to assess the safety of proposed changes. There are several current approaches being used or tried for NextGen. All involve the use of traditional hazard analysis techniques that are 40 to 50 years old and predate the extensive use of computers in complex systems. They do not handle the level of complexity underlying the plans for ATM upgrades and cannot be extended to do so because they are based on an underlying accident causal model that excludes the planned types of coupling and interconnectivity. The traditional hazard analysis techniques also are limited to completed designs and thus are not very useful in designing safety into the system from the beginning.

Our hypothesis is that these techniques miss the most important types of problems that are going to occur in a computer-intensive air traffic management system and that a totally different type of safety assessment paradigm is required. In this research, we will investigate an innovative and very different type of hazard analysis, based on systems theory rather than the traditional reliability theory underlying the other methods. The goal of this research is to (1) extend and demonstrate our new risk assessment paradigm for the problems that need to be solved to implement NextGen and (2) compare and evaluate the results with the current (traditional) hazard analysis techniques currently being used for NextGen.

More specifically, we will

1. Create a hazard analysis technique that is useful in the early concept design phase of NextGen operational increments and can be used to guide design decision making by engineers.
2. Devise a method to compare the risk involved in various alternative NextGen architectures.
3. Demonstrate how our new hazard analysis technique can be used to derive verifiable safety requirements and to derive scenarios for use in simulation environments.
4. Evaluate how the new approach would fit into the current FAA Safety Management System.
5. Include sophisticated human factors concepts in the new hazard analysis method
6. Evaluate the cost and work involved in using our new approach on upgrades in comparison with a more traditional hazard analysis. NextGen will involved phased rollout and mixed fleets, integration of UAVs, and starting from scratch in the hazard analysis will not be possible.
7. Compare the results of the new approach to the current one being used in highly-distributed, tightly coupled systems such as NextGen.